Privacy Charter

Prepared by

Hunter Macdonald, CEO and Tom Luke, VP Sales, Marketing and Alliances
Tutela Technologies Ltd.

Reviewed and approved, on the basis of a Privacy Impact Assessment, by

David H. Flaherty, Ph.D.
Privacy and Information Policy Consultant
David H. Flaherty Inc.

TUTELA

Tutela Privacy Charter

As a company whose livelihood depends on data and its proper treatment, Tutela takes data privacy very seriously. As such we have taken steps to go well beyond basic privacy requirements.

Tutela collects a lot of statistics and measurements, but we do not collect any identifiable personal information and we take steps to ensure that our datasets cannot be used to identify individual people or devices. We take these steps ourselves and also ensure that our data is treated in the same way by our customers and partners through strict licensing provisions.

Why we collect data.

We collect data so that we can help companies in the mobile industry understand their networks and understand trends in user and device behavior on aggregate. This is typically used to identify areas where there are poor WiFi or cellular signals.

The data we collect includes mobile signal strength, mobile connection quality, and performance of different mobile apps in different locations. All information is anonymous at all times.

Why we work with mobile apps and games partners.

Collecting data from millions of devices is difficult. Our research showed that users did not want to install more applications on their devices to collect data, but were happy to provide anonymous data if it helped to reduce advertisements, improve mobile signals, and if it did not affect their experience or device performance.

Our software runs in the background of popular mobile apps and games to collect data. This helps us to collect as much useful data as possible, without requiring the user to download another application. In many cases, this also means that the mobile apps can display fewer advertisements to users because we pay them to partner with us.

All of our mobile application and games partners are required to provide disclosures and permission requests to their users to enable anonymous data collection.

Our data is anonymous. We do not collect personal data.

We do not collect any identifiable personal data from users. In fact, our users are completely anonymous to us. We never collect name, email address, phone number, social media ID, or anything else which can identify a user. We also do not collect any identifying information about the device (e.g. serial number, MAC address).

Additionally we do not generate, use, collect or store a persistent internal device or Tutela ID to identify one of our installations. This helps to prevent the unlikely possibility of user attribution altogether. There is no ID to match data collected from a device one day with data collected from that same device any other day.

We transmit and store data securely. Safe from hacks and malicious attack.

We use the latest data security methods and premium data centers to ensure data is held securely. Our data is stored in databases encrypted using 2048 bit encryption and requires 2-factor authentication to be accessed.
When data is transferred from mobile devices to our database, we use 256 bit encryption.
We monitor the access to our databases carefully to identify any breach of security.

We are transparent about why we collect data and how we will use it.

We only use data to help companies improve their wireless networks, to identify trends in device and user behavior on aggregate, and to improve wireless security to further protect the privacy rights of consumers.

We only share data with trusted companies.

Our data is only shared with companies who agree to our strict privacy and data handling terms, or have their own equivalent privacy terms which they adhere to.
We take only the data we need.

We don't take more data than we need. We will only collect the data we need for our business.

We make it clear what you can opt-in and opt-out of.

Users are made aware that they are participating with the collection of anonymous statistics when running an application for the first time and have the option to opt-out. The procedure for doing this is generally found in their application terms of service and/or settings menu.

In special cases we allow users to opt-in to provide additional data to Tutela for advanced network troubleshooting. This data also does not contain any personal data and includes things like; when, where and why phone calls fail; providing IP address information.

Giving data will not negatively impact our users.

Providing data to us does not have any negative impact on users or their devices. Data we collect cannot be used to disadvantage our users. Quite the opposite; our data is typically used to improve mobile and WiFi networks to provide a better experience for users.

The impact to the device battery and CPU is designed and tested to be so small that it cannot be noticed by the average user (less than 1%). For our mobile application and game partners, the additional file size is less than 1 MB.

Our mobile app partners are anonymous too.

Our customers and partners cannot identify the mobile applications or publishers that our data has been received from. We collect data from over 100 different mobile applications but our reports, data and documentation do not reveal which mobile applications the source data was collected from. We do not publicly disclose our application partners without their permission.

National and State Data Protection Acts.

Tutela and its partners take reasonable steps to ensure compliance with government data protection legislation in the countries where it offers its services.

About David Harris Flaherty

David Flaherty is a specialist in the management of privacy and information policy issues. He served a six-year, non-renewable term as the first Information and Privacy Commissioner for the Province of British Columbia (1993-99).

As a consultant since 1999, Flaherty's services for clients have included strategic advice on the management of privacy issues and of relationships with privacy authorities, privacy advocates, and the general public; conducting overall assessments of privacy compliance (privacy reviews, audits, site visits, knowledge transfer); preparing Privacy Impact Assessments; helping to manage and prevent privacy breaches; and developing on-line privacy training and other privacy risk management tools.

David has been a member of both the External Advisory Committee to the Privacy Commissioner of Canada (from the Committee's inception in 2004 till his resignation in early June, 2014) and the expert external advisory board for the BC Office of the Information and Privacy Commissioner since its inception in January 2011. Since 2000, he has been the Chief Privacy Advisor to the Canadian Institute for Health Information (CIHI). He has also been a Director of MAXIMUS BC Health Inc. since its inception in 2005 as a service provider to the BC Ministry of Health Services through Health Information B.C.

In June, 2013 the Electronic Privacy Information Centre (EPIC) in Washington, DC honored Flaherty with a Lifetime Achievement Award for his work on privacy protection. In October, 2014 the Privacy and Access Council of Canada named him a Fellow, Access and Privacy Professional.